UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,239	09/12/2003	David D. Brandt	03AB014A/ALBRP303USA	6849

7590 08/13/2009

Susan M. Donahue
Rockwell Automation
704-P, IP Department
1201 South 2nd Street
Milwaukee, WI 53204

EXAMINER	
JARRETT, RYAN A	

ART UNIT	PAPER NUMBER
2121	

MAIL DATE	DELIVERY MODE
08/13/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/661,239	**Applicant(s)** BRANDT ET AL.	
	Examiner RYAN A. JARRETT	**Art Unit** 2121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2009*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-19,24,26,27 and 34-44* is/are pending in the application.

4a) Of the above claim(s) *24,26 and 27* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-19 and 34-44* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 June 2009* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *07/15/09*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 06/29/09 has been entered.

Drawings

The drawings were received on 06/29/09. These drawings are accepted.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 4-6, 9-19, and 34-44 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Batke et al. US 7,536,548.

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

For example, Batke et al. discloses:

1. An automation security system, comprising:

a processor operatively coupled to memory configured to support the operation of:

an asset component that defines an industrial automation device (e.g., col. 2 lines 35-49);

an access component that defines a security attribute associated with the industrial automation device, the security attribute including a location attribute and a time attribute, wherein the time attribute defines direct communication access to the industrial automation device for a predetermined amount of time (e.g., col. 10 line 59 – col. 11 line 26); and a security component that regulates initial and continuing direct communication access to the industrial automation device based upon the security attribute, wherein the security component monitors continuing direct communication and alters or discontinues direct communication access when a security issue arises or is detected (e.g., col. 9 lines 18-32: "After an SA has been establish…the IPSEC Driver may initiate re-keying based on duration lifetime, byte count lifetime, and/or policy changes, for example").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 4-6, and 9-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rammler US 2003/0105535 in view of Salowey US 7,370,350.

Rammler discloses:

1. An automation security system, comprising:

a processor operatively coupled to memory configured to support the operation of:

an asset component that defines an industrial automation device (e.g., [0185], [0327]);

an access component that defines a security attribute associated with the industrial automation device (e.g., [0196], [0230], [0232]), the security attribute including a location attribute (e.g., [0196]: "Access can be controlled…based on a valid IP address") ~~and a time attribute, wherein the time attribute defines direct communication access to the industrial automation device for a predetermined amount of time~~; and

a security component that regulates initial ~~and continuing~~ direct communication access to the industrial automation device based upon the security attribute (e.g., [0196]: "Access can be controlled…based on a valid IP address")~~, wherein the security component monitors continuing direct communication and alters or discontinues direct communication access when a security issue arises or is detected~~.

4. The system of claim 1, the security component is based on at least one of automation and process control security (e.g., [0184]-[0185]), cryptography, or Authentication/Authorization/Accounting (AAA).

5. The system of claim 1, the asset component describes at least one of factory components or groupings, the factory components are at least one of sensors, actuators, controllers, I/O modules, communications modules, or human-machine interface (HMI) devices (e.g., Figs. 5-8).

6. The system of claim 5, the groupings include factory components that are grouped into at least one of machines, machines grouped into lines, or lines grouped into facilities (e.g., Figs. 5-8).

9. The system of claim 1, further comprising a set of generic IT components and specification of values for parameters required to assemble and configure the IT components to achieve flexible access to the industrial automation device (e.g., Fig. 4, Fig. 6).

10. The system of claim 9, the IT components include at least one of switches with virtual local area network (VLAN) capability, routers with access list capability, firewalls, virtual private network (VPN) termination devices, intrusion detection systems, AAA servers, configuration tools, or monitoring tools (e.g., Fig. 4, Fig. 6).

11. The system of claim 1, further comprising security parameters and policies that are developed for physical and electronic security for various component types (e.g., [0196], [0230], [0232]).

12. The system of claim 11, the security parameters and policies further comprising at least one of integrity algorithms or privacy algorithms (e.g., [0196]: "Access can be controlled…based on a valid IP address", [0230], [0232]).

13. The system of claim 1, the security component includes at least one of authentication software, virus detection, intrusion detection, authorization software (e.g., [0196], [0230], [0232]), attack detection, protocol checker, or encryption software.

14. The system of claim 13, the security component at least one of acts as an intermediary between an access system and one or more automation components, or facilitates communications between the access system and the one or more automation components (e.g., Fig. 4, Fig. 6).

15. The system of claim 1, the security attributes are specified as part of a network request to gain access to the at least one industrial automation device, the security attributes included in at least one of a group, set, subset, or class (e.g., Fig. 4, Fig. 6, [0196], [0230], [0232]).

16. The system of claim 15, the security component employs at least one authentication procedure or an authorization procedure to process the network request (e.g., [0196], [0230], [0232]).

17. The system of claim 16, further comprising one or more security protocols including at least one of Internet Protocol Security (IPSec), Kerberos, Diffie-Hellman exchange, Internet Key Exchange (IKE), digital certificate, pre-shared key, or encrypted password, to process the network request (e.g., [0060], [0187]).

18. The system of claim 15, further comprising a security switch to control network access to a device or network (e.g., Fig. 4, Fig. 6, [0060], [0187]).

19. The system of claim 18, the access key further comprises at least one of time, location, batch, process, program, calendar, or GPS (Global Positioning Information) to specify local and wireless network locations, to control access to the device or network (e.g., Fig. 4, Fig. 6, [0060], [0187], [0196], [0230], [0232]).

Rammler does not explicitly disclose a time attribute, wherein the time attribute defines direct communication access to the industrial automation device for a predetermined amount of time; wherein the security component monitors continuing direct communication and alters or discontinues direct communication access when a security issue arises or is detected, as recited in claim 1.

Rammler does disclose a timeout feature (e.g., [0190]), but it does not appear to be in the context of granting access to a device for a predetermined amount of time.

Salowey US 7,370,350 discloses a method and apparatus for re-authentication computing devices, comprising a time attribute, wherein the time attribute defines direct communication access to the industrial automation device for a predetermined amount of time; wherein the security component monitors continuing direct communication and alters or discontinues direct communication access when a security issue arises or is detected (e.g., col. 7 lines 33-49, *The detected "security issue" is the expiration date/time. Salowey monitors the particular connection and determines the expiration date/time for that connection. When the expiration date/time arrives, the connection expires or discontinues.*).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Rammler with Salowey since all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention. See KSR v. Teleflex, 127 S.Ct. 1727 (2007).

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rammler as modified by Salowey (or just Batke et al.) as applied to claim 5 above, and further in view of Hammer et al. US 2008/0016569.

Rammler as modified by Salowey does not appear to explicitly disclose that the groupings have associated severity attributes including at least one of risk and security incident cost.

Hammer et al. discloses a system for managing one or more security incidents and/or potential security incidents, wherein the potential security incidents include severity attributes including at least one of risk and security incident cost (e.g., [0015], [0097]).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Rammler as modified by Salowey (or just Batke et al.) with Hammer et al. since all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention. See KSR v. Teleflex, 127 S.Ct. 1727 (2007).

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rammler as modified by Salowey and Hammer et al. (or just Batke in view of Hammer et al.) as applied to claim 7 above, and further in view of Schleiss et al. US 2003/0014500.

Rammler as modified by Salowey and Hammer et al. (or just Batke in view of Hammer et al.) does not appear to explicitly disclose an ISA S95 Model for Enterprise to Control System Integration to integrate security aspects across or within respective groupings.

Schleiss et al. discloses ISA S95 Model for Enterprise to Control System Integration to integrate security aspects across or within respective groupings (e.g., [0007]-[0008], [0053]).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Rammler as modified by Salowey and Hammer et al. (or just Batke in view of Hammer et al.) with Schleiss et al. since all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention. See KSR v. Teleflex, 127 S.Ct. 1727 (2007).

Response to Arguments

Applicant's arguments filed 06/29/09 have been fully considered but they are not fully persuasive. Examiner agrees that primary reference Rammler does not disclose the amended features of claim 1, but asserts that they are taught by secondary reference Salowey. In Salowey, the detected "security issue" is the expiration date/time. Salowey monitors the particular connection and determines the expiration date/time for that connection. When the expiration date/time arrives, the connection expires or discontinues.

Regarding claim 12, integrity and privacy algorithms are broad terms and read on the authentication/authorization algorithms of Rammler.

Regarding claim 18, Rammler discloses a security router/switch in the cited Figures.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RYAN A. JARRETT whose telephone number is (571)272-3742. The examiner can normally be reached on 10:00-6:30 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ryan A. Jarrett/
Primary Examiner, Art Unit 2121

08/11/09